(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
18 décembre 2003 (18.12.2003)

PCT

(10) Numéro de publication internationale
WO 03/105399 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR03/01535

(22) Date de dépôt international : 21 mai 2003 (21.05.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/06915 5 juin 2002 (05.06.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **PAILLES, Jean-Claude** [FR/FR]; 4, rue des Loisirs, F-14610 Epron (FR). **BOUTROUX, Vincent** [FR/FR]; 229, rue Jean-Moulin, F-14880 Hermanville sur Mer (FR).

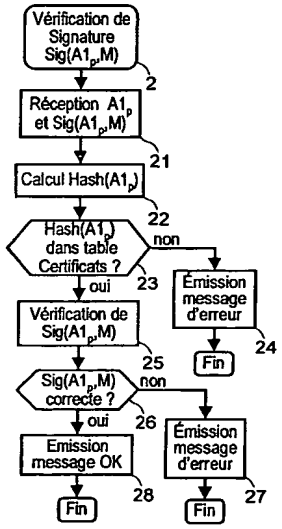
(74) Mandataires : **DE ROQUEMAUREL, Bruno** etc.; Novagraaf Technologies, 122, rue Edouard Vaillant, F-92593 Levallois Perret Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR VERIFYING ELECTRONIC SIGNATURES AND MICROCIRCUIT CARD FOR CARRYING OUT SAID METHOD

(54) Titre : PROCEDE ET SYSTEME DE VERIFICATION DE SIGNATURES ELECTRONIQUES ET CARTE A MICROCIRCUIT POUR LA MISE EN ŒUVRE DU PROCEDE



2 VERIFY SIGNATURE (SIG(A1$_P$,M))
21 RECEIVE A1$_P$ AND S$_{IG}$(A1$_P$,M))
22 CALCULATE HASH(A1$_P$)
23 HASH(A1$_P$) IN TABLE OF CERTIFICATES?
NON NO
OUI YES
24, 27 EMIT ERROR MESSAGE
FIN END
25 VERIFY SIG(A1$_P$,M)
26 SIG(A1$_P$,M) CORRECT?
28 EMIT MESSAGE OK

(57) **Abstract:** Disclosed is a method for verifying an electronic signature by means of a microcircuit card, said microcircuit receiving and processing requests for electronic signature verifications. The inventive method comprises a stage in which a table of certificates containing condensed forms of authorized public keys is stored in a memory of the microcircuit, and an electronic signature verification phase (2) which consists of: the microcircuit receiving (21) the electronic signature (Sig(A1$_p$,M)) that is to be verified and a public key (A1$_p$) corresponding to the private key that is used for creating the electronic signature; calculating (22) a condensed form (Hash(A1$_p$)) of the received public key; looking (23) for the condensed form of the public key within the table of certificates; and deciphering (25) the electronic signature by means of the received public key if the condensed form of the public key is included in the table of certificates.

(57) **Abrégé :** Pour vérifier une signature électronique à l'aide d'une carte à microcircuit, le microcircuit étant conçu pour recevoir et traiter des demandes de vérification de signatures électroniques, ce procédé comprend le stockage dans un mémoire du microcircuit d'une table de certificats contenant des formes condensées de clés publiques autorisées, et une phase (2) de vérification d'une signature électronique consistant à : recevoir (21) par le microcircuit la signature électronique (Sig(A1<sb>p</sb>, M)) à vérifier et une clé publique (A1<sb>p</sb>) correspondant à la clé privée utilisée pour générer la signature électronique ; calculer (22) une forme condensée (Hash(A1<sb>p</sb>)) de la clé publique reçue ; rechercher (23) dans la table de certificats la forme condensée de la clé publique ; et de déchiffrer (25) la signature électronique à l'aide de la clé publique reçue si la forme condensée de clé la publique se trouve dans la table de certificats.

WO 03/105399 A1

SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE ET SYSTEME DE VERIFICATION DE SIGNATURES ELECTRONIQUES ET CARTE A MICROCIRCUIT POUR LA MISE EN ŒUVRE DU PROCEDE.

La présente invention concerne un procédé et un système de vérification de signatures électroniques et une carte à microcircuit permettant la mise en œuvre de ce procédé.

Elle s'applique notamment, mais non exclusivement, à l'authentification d'informations, et à la vérification de signatures électroniques en vue d'autoriser certains traitements. Ces traitements consistent notamment à enregistrer des droits dans une carte à microcircuit électronique, par exemple dans des applications de ticket électronique de transport, ou de porte-monnaie électronique, ou encore de distribution de bons de réduction.

En effet, les cartes à microcircuit électronique, dites cartes à puce, sont utilisées généralement comme support informatique mobile pour des applications très diverses et exigeant pour la plupart d'entre elles un haut niveau de sécurité, notamment les opérations bancaires, les paiements sécurisés, l'accès aux bâtiments ou à des zones sécurisées et les télécommunications.

Lorsque l'on souhaite par exemple mettre à jour dans une carte à puce des données sensibles telles qu'un montant de recharge dans le cadre d'une application de porte-monnaie électronique, il est nécessaire que la carte soit en mesure de contrôler l'origine d'un ordre de mise à jour qu'elle reçoit. A cet effet, l'ordre de mise à jour est associé à une signature électronique dont l'identité du signataire est garantie par un certificat qui est également associé avec l'ordre de mise à jour.

Une signature électronique apposée sur un message est en général obtenue en appliquant une fonction de hachage au message pour en obtenir un condensé et en chiffrant ce condensé à l'aide d'une clé privée connue seulement du signataire. Pour vérifier une signature, il suffit donc de disposer de la clé publique correspondant à la clé privée utilisée, ainsi que de la fonction de hachage, d'appliquer la fonction de hachage au message, de déchiffrer la signature à l'aide de la clé publique, et de comparer le résultat fourni par la fonction de hachage avec le résultat fourni par le déchiffrement. Si ces deux

résultats sont identiques, la signature est correcte.

Un certificat de clé publique, par exemple conforme à la norme X509 ou PKCS#6, est constitué de l'association d'une clé publique utilisée par une personne, d'informations d'identification de cette personne et de la définition d'une période de validité, l'association de ces informations étant rendue infalsifiable par une signature électronique apposée par une autorité de certification, cette signature utilisant une clé privée de l'autorité de certification. Pour vérifier un certificat, il suffit de disposer de la clé publique de l'autorité de certification correspondant à la clé privée utilisée, et d'utiliser cette clé publique pour contrôler que la signature électronique émane bien de l'autorité de certification. On peut ainsi s'assurer qu'une clé publique correspond à l'identité d'une personne déterminée. Toutefois, ce principe ne garantit pas que la personne qui utilise la clé privée correspondant à la clé publique est bien à celle identifiée dans le certificat. En général, les autorités de certification ne garantissent pas cette correspondance.

Pour garantir une telle correspondance, on a déjà proposé de mettre en place une organisation en chaîne ou pyramidale basée sur le concept de "chaînes de certificats" dans laquelle la signature électronique de chaque personne est certifiée par la signature d'une entité qui a été préalablement certifiée par une autre entité, et ainsi de suite jusqu'à une autorité de référence située au sommet de la pyramide. Dans une telle organisation, une signature s'appuie sur tous les certificats de toutes les clés publiques permettant de remonter la chaîne de certification jusqu'à l'autorité de référence. Pour vérifier une signature, il faut donc vérifier tous les certificats jusqu'à un certificat délivré par une entité connue dans la chaîne de certification. Il faut en outre que la clé publique de cette entité connue soit stockée d'une manière sûre et infalsifiable.

Les techniques à mettre en œuvre pour gérer une telle organisation peuvent être facilement implantées dans un ordinateur personnel de type PC, notamment par l'intermédiaire de logiciels de navigation Internet qui intègrent tout ou partie de ces fonctions avec les protocoles SSL ("Secure Sockets Layer") et HTTPS ("Hypertext Transfer Protocol" intégrant SSL). Par contre, elles sont beaucoup plus difficiles à mettre en œuvre dans une carte à puce qui possède une puissance de calcul et des capacités de stockage notablement plus limitées. En effet, les chaînes de certificats qu'il faut traiter sont très longues par rapport aux caractéristiques habituelles des cartes à puces. Ainsi, un certificat conforme à la

norme X509 peut atteindre quelques kilo bits, et si la chaîne de certificats est longue, la carte doit pouvoir traiter et mémoriser une quantité d'informations trop importante par rapport à ses capacités.

Il convient de souligner à ce sujet qu'il n'est pas possible sans affecter la sécurité de faire exécuter de tels traitements par le terminal auquel la carte à puce est connectée ou d'utiliser la mémoire du terminal, car il serait alors facile de tromper la carte, notamment en changeant une clé publique par une autre.

On a déjà proposé d'introduire dans la mémoire de la carte à puce toutes les clés publiques des autorités de certification de la chaîne de certification. Toutefois, cette solution nécessite des capacités de mémoire importantes, compte tenu qu'une clé publique atteint couramment plus de un kilo bits. Il est en outre nécessaire que ces clés publiques soient stockées dans une zone mémoire sécurisée, pour éviter les risques de fraude consistant à introduire dans cette liste de clés publiques une clé non autorisée. Il s'avère qu'à l'heure actuelle, les microcircuits implantés dans les cartes à puce ne disposent pas d'autant de capacité mémoire sécurisée.

La présente invention a pour but de supprimer ces inconvénients en proposant une organisation de données et de traitements entre une carte à puce et un terminal, permettant de minimiser les contraintes appliquées à la carte en termes de quantité de mémoire et de traitements nécessaires, sans pour autant affecter la sécurité du système dans lequel ils sont mis en œuvre. Cet objectif est atteint par la prévision d'un procédé de vérification d'une signature électronique, faisant intervenir un microcircuit connectable à un système de traitement de données, le microcircuit étant conçu pour recevoir du système de traitement de données, des demandes de vérification de signatures électroniques et traiter ces demandes, une signature électronique étant générée à l'aide d'une clé privée connue seulement d'une entité signataire et associée à une clé publique.

Selon l'invention, ce procédé comprend une étape de stockage dans une mémoire du microcircuit d'une table de certificats contenant une forme condensée d'au moins une clé publique, et une phase de vérification d'une signature électronique comportant les étapes consistant à :

- recevoir par le microcircuit la signature électronique à vérifier et une clé publique d'une paire de clés comprenant une clé privée ayant été utilisée pour générer la signature électronique à vérifier,
- calculer une forme condensée de la clé publique reçue, et rechercher dans la

table de certificats la forme condensée calculée de la clé publique, et
- déchiffrer la signature électronique à l'aide de la clé publique reçue si la forme condensée calculée de la clé publique se trouve dans la table de certificats.

Selon une particularité de l'invention, ce procédé comporte une phase d'insertion d'une clé publique dans la table de certificats, comprenant les étapes consistant à :

- recevoir par le microcircuit un certificat de la clé publique à insérer dans la table de certificats, et une clé publique d'une entité de certification ayant généré le certificat, le certificat comprenant la clé publique à ajouter dans la table de certificats et une signature électronique de l'entité de certification, générée à l'aide d'une clé privée appartenant à une paire de clés comprenant la clé publique de l'entité de certification,
- calculer par le microcircuit une forme condensée de la clé publique reçue de l'entité de certification, et rechercher dans la table de certificats la forme condensée calculée de la clé publique,
- déchiffrer la signature électronique à l'aide de la clé publique reçue de l'entité de certification si la forme condensée calculée de la clé publique se trouve dans la table,
- extraire du certificat la clé publique à insérer si la signature électronique déchiffrée est correcte,
- calculer un condensé de la clé publique extraite du certificat et insérer le condensé calculé dans la table de certificats.

Avantageusement, la phase d'insertion d'une clé publique dans la table de certificats comprend l'insertion, en association avec le condensé inséré de la clé publique, d'un pointeur dans la table de certificats vers le condensé de la clé publique de l'entité de certification qui a émis le certificat de la clé publique à insérer, de manière à définir un arbre de certification.

Selon une autre particularité de l'invention, ce procédé comprend une phase de suppression d'un condensé de clé publique dans la table de certificats consistant à supprimer de la table de certificats le condensé d'une clé publique à retirer, et à supprimer tous les condensés de clés publiques de la table de certificats associés à un pointeur indiquant la clé publique à retirer.

De préférence, chaque condensé de clé publique inscrit dans la table de certificats est associé à une date de fin de validité, et en ce que la phase d'insertion d'une clé publique dans la table de certificats comprend en outre des étapes consistant à lire dans le certificat reçu une date de fin de validité de la clé publique à insérer, et à inscrire dans la table de certificats, en association avec le condensé de la clé publique à insérer, la date de fin de validité de la clé publique à insérer, si elle est antérieure à la date de fin de validité de la clé publique de l'entité de certification lue dans la table de certificats.

Egalement de préférence, chaque condensé de clé publique inscrit dans la table de certificats est associé à un compteur d'utilisation qui est incrémenté à chaque fois qu'une signature électronique est vérifiée à l'aide de la clé publique, et en ce qu'il comprend la suppression d'un condensé de clé publique dans la table de certificats lorsque le compteur d'utilisation est nul et que le nombre d'emplacements vides dans la table de certificats est inférieur à un seuil prédéterminé.

Egalement de préférence, chaque condensé de clé publique inscrit dans la table de certificats est associé à un compteur d'utilisation qui est incrémenté à chaque fois qu'une signature électronique est vérifiée à l'aide de la clé publique, à une date de dernière utilisation qui est mise à jour à chaque fois que le compteur d'utilisation associé est incrémenté, et en ce que lorsque le nombre d'emplacements vides dans la table de certificats est inférieur à un seuil prédéterminé, il comprend en outre une étape de sélection d'un condensé de clé publique à supprimer en fonction des valeurs respectives associées du compteur d'utilisation et de la date de dernière utilisation.

Avantageusement, le microcircuit utilise une fonction de hachage prédéfinie pour calculer des formes condensées de clés publiques.

Selon encore une autre particularité de l'invention, ce procédé comporte une phase d'insertion d'une clé publique racine dans la table de certificats, cette phase d'insertion étant effectuée par un traitement d'écriture contrôlée par un MAC calculé à l'aide d'une clé spécifique du microcircuit et connue uniquement d'une entité émettrice du microcircuit.

Avantageusement, le condensé d'une clé publique mémorisé dans la table de certificats est obtenu en calculant un condensé de la clé publique associée à

d'autres informations comme la date de fin de validité de la clé publique, des informations d'identité, et de numéros de série, ces informations étant transmises au microcircuit à chaque vérification de signature à l'aide de la clé publique.

Avantageusement, le condensé d'une clé publique mémorisé dans la table de certificats est obtenu en calculant un condensé du certificat reçu par le microcircuit lors de l'insertion de la clé publique dans la table de certificats, ce certificat étant transmis au microcircuit à chaque vérification de signature à l'aide de la clé publique.

De préférence, la table de certificats est stockée dans une zone mémoire sécurisée du microcircuit.

L'invention concerne également une carte à microcircuit mettant en œuvre le procédé défini ci-avant.

L'invention concerne également un système de vérification de signature électronique comprenant un microcircuit connectable à un système de traitement de données, pour la mise en œuvre du procédé défini ci-avant.

Un mode de réalisation préféré de l'invention sera décrit ci-après, à titre d'exemple non limitatif, avec référence aux dessins annexés dans lesquels :

La figure 1 représente schématiquement un système dans lequel le procédé selon l'invention peut être mis en œuvre ;

La figure 2 représente un arbre de certificats ;

La figure 3 représente une table de certificats telle qu'elle est mémorisée dans une carte à puce, selon l'invention ;

Les figures 4 à 6 représentent sous la forme d'organigrammes de différentes procédures qui sont exécutées par une carte à puce, selon l'invention ;

La figure 7 représente une variante selon l'invention de la table de certificats représentée sur la figure 3.

Le système représenté sur la figure 1 comprend une pluralité de terminaux 51 connectés à des réseaux 50 de transmission de données numériques. Ces terminaux sont conçus pour fournir différents services nécessitant d'être protégés contre les fraudes, tels que le rechargement de portes-monnaie électroniques, ou l'attribution d'un droit (par exemple de transport), ou encore pour l'échange sécurisé de données.

Par ailleurs, les utilisateurs du système disposent d'une carte personnelle, de type carte à microprocesseur 53, plus couramment appelée carte à puce, chaque terminal 51 étant équipé de moyens de communication 52, tels qu'un lecteur de carte à puce, pour communiquer avec le microprocesseur de la carte 53.

Pour qu'un utilisateur puisse accéder à un service tel que mentionné ci-avant, il doit posséder une carte à puce 53 dans laquelle se trouve mémorisé une clé publique attribuée au service. Cette clé publique lui permet de vérifier ou d'authentifier les signatures des différents terminaux grâce à une chaîne de certification.

La figure 2 représente un arbre de certificats de clés publiques comprenant plusieurs chaînes de certification. Cet arbre montre par des liens entre des clés que les clés publiques respectives d'entités A1 et A2 sont certifiées par une entité A, et que les clés publiques de l'entité A et d'une entité B sont certifiées par une entité R appelée "racine" du fait qu'elle est située à la racine de l'arbre.

Si l'on souhaite qu'un certificat émis par exemple par l'entité A2 et portant sur une clé publique d'une personne X, puisse être vérifié par une personne ne connaissant que l'autorité de certification R, il est nécessaire de lui transmettre l'ensemble d'une chaîne de certificats comprenant un certificat émis par l'autorité de certification R. Si l'on note <A,A1> un certificat émis par l'entité A et portant sur la clé publique d'une entité A1, une telle chaîne de certification est constituée des certificats suivants :

$$<A2,X><A,A2><R,A>.$$

Chaque certificat est constitué de la signature de l'autorité de certification apposée sur la clé publique à certifier, associée à des informations d'identification du titulaire de la clé publique à certifier et de l'autorité de certification, et éventuellement à des dates de début et de fin de validité. On a donc $<R,A> = (Sig_R(A_p$, Identité de A, Dates de début et de fin de validité), Identité de R), A_p représentant la clé publique de l'entité A.

Si dans l'exemple précédent, on souhaite qu'une signature $Sig_X(M)$ émise par la personne X et portant sur un message M, puisse être vérifiée par une personne ne connaissant que l'autorité de certification R, il est nécessaire d'associer à cette signature les certificats mentionnés précédemment :

$$Sig_X(M)<A2,X><A,A2><R,A>$$

De cette manière, si l'on connaît la clé publique R_p, le certificat <R,A> fournit la clé publique A_p de l'entité A. Le certificat <A,A2> fournit la clé publique $A2_p$ de l'entité A2, et le certificat <A2,X> fournit la clé publique X_p permettant de vérifier la signature $Sig_X(M)$.

Lorsque l'on souhaite vérifier une signature et donc s'assurer de la validité d'une clé publique, ce processus implique la transmission d'une quantité importante d'informations et de nombreux traitements, ces contraintes étant incompatibles avec les capacités de stockage et de traitement d'une carte à puce.

Pour résoudre ce problème, la présente invention prévoit de stocker dans la mémoire de la puce, non pas les clés publiques des autorités de certification reconnues, mais un condensé de ces clés publiques, obtenu par exemple à l'aide d'une fonction dite de hachage, telle que MD4 ou 5 ("Message Digest"), SHA ("Secure Hash Algorithm") ou HMAC ("Hashed Message Authentication Code").
Ces clés condensées sont stockées sous la forme d'une table de certificats 5 telle que représentée sur la figure 3. Dans la table de certificats représentée sur cette figure, chaque condensé de clé publique $Hash(X_p)$ 6 est associé à une date de fin de validité 7 du certificat correspondant, par exemple définie sous la forme <numéro de mois>/<année sur 2 chiffres>, et un pointeur 8 vers la ligne du tableau correspondant à la clé publique située en amont dans la chaîne de certification.

Ainsi, par exemple la clé $A2_p$ mémorisée sous forme condensée à la quatrième ligne du tableau est associé à une date de fin de validité égale à décembre 2002 et est rattachée à la ligne 2 du tableau dans laquelle se trouvent mémorisées les informations concernant la clé publique A_p. D'une manière générale, les pointeurs figurant dans la colonne de pointeurs 8 de la table 5 permettent donc

de reconstituer l'arbre de certification représenté sur la figure 2.

Comme la clé racine R_p de l'arbre de certification n'est rattachée à aucune autre clé, elle est associée dans la table de certification à un pointeur nul.

Bien entendu, la table de certification selon l'invention peut contenir plusieurs arbres de certification indépendants, et donc plusieurs clés racine.

Outre le fait qu'elle réduit les ressources mémoire nécessaires, l'invention permet également de simplifier la gestion de cette mémoire sachant que la taille des clés est variable (elle est en général plus importante pour les clés racine que pour les autres clés), et qu'une fonction de hachage fournit une séquence binaire d'une longueur constante quelle que soit la taille de la séquence binaire appliquée en entrée de la fonction.

Conformément à l'invention, cette table de certificats 5 est associée à une procédure d'insertion d'une nouvelle clé certifiée par une clé figurant dans la table, une procédure de suppression d'une clé de la table, et une procédure de vérification de signature ayant utilisé une clé de la table, ces procédures étant stockées dans la mémoire programme de la carte à puce 53 et étant exécutables par l'unité de traitement de la carte, sur commande du terminal 51 relié à la carte.

L'insertion d'une nouvelle clé dans la table de certificats 5 est effectuée par une procédure 1 illustrée schématiquement dans la figure 4.

A l'étape 10, cette procédure reçoit le certificat de la clé publique à insérer dans la table 5, <R,B> dans l'exemple représenté, associé à la clé publique R_p de l'autorité de certification qui a émis le certificat. A l'étape suivante 11, cette procédure calcule un condensé Hash(R_p) de la clé publique reçue R_p à l'aide d'une fonction de hachage prédéfinie, puis recherche 12 dans la table de certificats ce condensé de clé. Si ce condensé de clé Hash(R_p) ne figure pas dans la table de certificats 5, cette procédure renvoie 13 en réponse un message d'erreur. Dans le cas contraire, elle vérifie 14 le certificat en tentant de le déchiffrer à l'aide de la clé publique R_p. Si ce certificat n'est pas valide, c'est-à-dire s'il ne peut pas être déchiffré à l'aide de la clé publique R_p (étape 15), cette procédure renvoie 16 en réponse un message d'erreur. Dans le cas contraire, elle extrait 17 du certificat <R,B> la clé publique B_p à insérer dans la table de

certificats, puis elle calcule 18 un condensé Hash(B_p) de cette clé publique à l'aide de la même fonction de hachage, et insère 19 la clé publique condensée obtenue dans la table de certificats. A l'étape 19, la procédure insère également dans la table 5 la date de fin de validité fournie par le certificat <R,B>, et insère dans la colonne 8 des pointeurs de la table de certificats, l'adresse ou le numéro de la ligne de la table correspondant à la clé publique R_p fournie avec le certificat <R,B> en entrée de la procédure, cette adresse ou ce numéro de ligne ayant par exemple été mémorisé à l'étape 12.

Lors de l'étape d'insertion de la nouvelle clé B_p dans la table, on peut s'assurer au préalable que la date de fin de validité de la nouvelle clé est antérieure à la date de fin de validité de la clé R_p à laquelle elle est rattachée par le certificat. Cette disposition vise à satisfaire le principe qu'une autorité ne peut pas attribuer des droits plus étendus que ceux dont elle dispose. Si cette date est postérieure à la date de fin de validité de la clé à laquelle elle est rattachée, on peut prévoir d'inscrire dans la table, la date la plus ancienne parmi ces deux dates. En variante, on peut décider pour des raisons de sécurité de ne pas inscrire la nouvelle clé dans la table et d'émettre un message d'erreur à destination du terminal.

La procédure 1 qui vient d'être décrite permet donc d'insérer dans la table une clé rattachée par un certificat à une autre clé dont le condensé se trouve déjà dans la table de certificats 5. Toute la sécurité du système de certification mis en œuvre par la table de certificats et la procédure d'insertion d'une nouvelle clé dans la table, repose donc sur la procédure employée pour insérer une clé racine dans la table. Pour cette raison, l'insertion d'une clé racine doit être effectuée par une procédure assurant une protection suffisante. A cet effet, une telle procédure peut par exemple comprendre un traitement classique d'écriture contrôlée par un MAC (Message Authentication Code") calculé à l'aide d'une clé spécifique de la carte et connue uniquement de l'émetteur de la carte.

La figure 5 illustre schématiquement la procédure 2 de vérification de signature notée Sig(A_p,M) pour indiquer qu'elle est apposée au message M et a été générée à l'aide d'une clé privée correspondant à la clé publique A_p.

Cette procédure reçoit en entrée à l'étape 21 la signature à vérifier, par exemple Sig($A1_p$,M) et la clé publique $A1_p$ correspondant à la clé privée ayant été utilisée pour générer la signature.

A l'étape 22, cette procédure calcule un condensé Hash($A1_p$) de la clé $A1_p$ reçue, et à l'étape 23 recherche si ce condensé de clé se trouve dans la table de certificats 5. S'il ne s'y trouve pas, la carte ne peut pas vérifier la signature et retourne 24 un message d'erreur. Dans le cas contraire, elle vérifie 25 la signature en tenant de déchiffrer le condensé du message M à l'aide de la clé publique $A1_p$. Aux étapes suivantes 26, 27, 28, elle retourne un message donnant le résultat de la vérification.

La figure 6 illustre schématiquement la procédure 3 de retrait d'une clé de la table de certificats 5. A l'étape 31, cette procédure reçoit en entrée la clé B_p à supprimer. Aux étapes 32 et 33, cette procédure calcule le condensé Hash(B_p) de la clé B_p et recherche le condensé de cette clé dans la table 5. Si la clé à supprimer n'est pas trouvée dans la table, cette procédure retourne 34 un message d'erreur. Dans le cas contraire, elle supprime toutes les informations figurant dans la ligne trouvée de la table 5. A l'étape suivante 36, elle recherche si d'autres clés doivent être retirées de la table 5 du fait qu'elles sont rattachées à la clé supprimée, c'est-à-dire si la table contient des pointeurs indiquant la ligne supprimée. Si d'autres clés doivent être supprimées (étape 37) de la table, cette procédure passe à l'étape 38 consistant à exécuter la procédure 3 à partir de l'étape 35 pour chacune des clés trouvées. De cette manière, si on retire la clé A de la table, on retire également, d'une manière automatique toutes les clés rattachées à A, c'est-à-dire dans l'exemple de la figure 2, les clés A1 et A2, ainsi que toutes les clés qui seraient rattachées à A1 ou A2.

Il est à noter que la procédure 3 peut être appelée régulièrement par l'unité de traitement de la carte, par exemple lorsque celle-ci reçoit la date courante, pour retirer de la table 5 toutes les clés qui ont expiré, c'est-à-dire qui ont une date de fin de validité antérieure à la date courante.

En outre, en fin de traitement de suppression, on peut prévoir de réorganiser la table 5 en décalant toutes les lignes non vides de la table vers le début de celle-ci de manière à éliminer toutes les lignes vides entre deux lignes non vides.

On peut remarquer que les procédures 1, 2, 3 qui viennent d'être décrites peuvent être exécutées en mode non connecté, c'est-à-dire qu'elles ne nécessitent pas l'intervention d'autres entités que la carte à puce 53 et le terminal 51 auquel celle-ci est raccordée, dès lors que le terminal dispose des certificats, signatures et clés publiques requis par ces procédures.

On peut également prévoir dans la table des certificats 5' une colonne 41 supplémentaire, destinée à recevoir des compteurs d'utilisation associés à chaque clé de la table (figure 7).

A chaque fois que la procédure 2 est exécutée pour vérifier une signature à partir d'une clé de la table, on incrémente de 1 le compteur correspondant, lequel a été initialisé à 0 lors de l'insertion de la clé dans la table, ainsi que tous les compteurs associés aux clés appartenant à la même chaîne de certification, situées en amont, c'est-à-dire entre la clé correspondant à la signature vérifiée et la clé racine de la chaîne de certification. A titre d'exemple, si la procédure 2 est appelée pour vérifier une signature à l'aide de la clé $A1_p$, les compteurs associés aux clés $A1_p$, A_p et R_p sont incrémentés.

Cette disposition permet de gérer plus efficacement la mémoire de la carte à puce 53 qui est limitée, en donnant une information sur l'utilisation de chaque clé de la table de certification en vue de retirer de la table de certification les clés qui n'ont jamais été utilisées. Le déclenchement de ce retrait peut être effectué le terminal 51. Dans ce cas, la procédure 1 comprend une étape d'émission d'un message "mémoire insuffisante" à destination du terminal lorsque le nombre de lignes vides de la table 5' est inférieur à un nombre prédéfini. On peut également prévoir que la procédure 1 déclenche ce retrait en en appelant la procédure 3 à l'étape 19.

Par ailleurs, si tous les compteurs de la table 5' sont non nuls et que la table est pleine, on peut prévoir de supprimer la clé associée à la valeur de compteur la plus faible. Si plusieurs clés dans la table 5' répondent à ce critère, la clé qui est choisie pour être retirée de la table peut être l'une de celles qui sont les plus éloignées d'une clé racine.

En outre, la table peut contenir une colonne 42 supplémentaire contenant la date de mise à jour de chaque compteur ou date de la dernière utilisation de la clé. De cette manière, on peut combiner un critère de nombre d'utilisation et un critère de date de dernière utilisation, ou appliquer l'un ou l'autre de ces deux critères pour sélectionner les clés à retirer de la table de certificats 5'. Selon les applications, on peut ainsi choisir de supprimer de la table la clé associée à une date de dernière utilisation la plus ancienne.

La table de certificats selon l'invention peut mémoriser d'autres informations

sous forme condensée, telle que des informations d'identité, de numéro de série, de date de fin de validité, etc. Dans ce cas, ces informations doivent être transmises à la carte lors de l'appel des procédures 1, 2 et 3.

Selon une variante de l'invention, la table mémorise non pas un condensé des clés publiques des autorités de certification, mais un condensé de certificats émis par ces dernières et constituant l'arbre de certification. Ces certificats doivent alors être transmis à la carte lors de l'appel des procédures 1, 2 et 3.

REVENDICATIONS

1. Procédé de vérification d'une signature électronique, faisant intervenir un microcircuit (53) connectable à un système de traitement de données (51), le microcircuit étant conçu pour recevoir du système de traitement de données, des demandes de vérification de signatures électroniques et traiter ces demandes, une signature électronique étant générée à l'aide d'une clé privée connue seulement d'une entité signataire et associée à une clé publique,
caractérisé en ce qu'il comprend une étape de stockage dans une mémoire du microcircuit (53) d'une table de certificats (5, 5') contenant une forme condensée d'au moins une clé publique, et une phase (2) de vérification d'une signature électronique comportant les étapes consistant à :
- recevoir (21) par le microcircuit la signature électronique ($Sig(A1_p,M)$) à vérifier et une clé publique ($A1_p$) d'une paire de clés comprenant une clé privée ayant été utilisée pour générer la signature électronique à vérifier,
- calculer (22) une forme condensée ($Hash(A1_p)$) de la clé publique reçue, et rechercher (23) dans la table de certificats (5, 5') la forme condensée calculée de la clé publique, et
- déchiffrer (25) la signature électronique à l'aide de la clé publique reçue si la forme condensée calculée de la clé publique se trouve dans la table de certificats.

2. Procédé selon la revendication 1,
caractérisé en ce qu'il comporte une phase (1) d'insertion d'une clé publique (B_p) dans la table de certificats (5, 5'), comprenant les étapes consistant à :
- recevoir (10) par le microcircuit (53) un certificat (<R,B>) de la clé publique (B_p) à insérer dans la table de certificats, et une clé publique (R_p) d'une entité de certification ayant généré le certificat, le certificat comprenant la clé publique à ajouter dans la table de certificats et une signature électronique de l'entité de certification, générée à l'aide d'une clé privée appartenant à une paire de clés comprenant la clé publique de l'entité de certification,
- calculer (11) par le microcircuit une forme condensée ($Hash(R_p)$) de la clé publique (R_p) reçue de l'entité de certification, et rechercher (12) dans la table de certificats la forme condensée calculée de la clé publique,
- déchiffrer (14) la signature électronique à l'aide de la clé publique reçue de l'entité de certification si la forme condensée calculée de la clé publique se trouve dans la table,

- extraire (17) du certificat la clé publique (B_p) à insérer si la signature électronique déchiffrée est correcte,
- calculer (18) un condensé (Hash(B_p)) de la clé publique (B_p) extraite du certificat et insérer (19) le condensé calculé dans la table de certificats.

3. Procédé selon la revendication 2,
caractérisé en ce que la phase (1) d'insertion d'une clé publique (B_p) dans la table de certificats (5, 5') comprend l'insertion, en association avec le condensé inséré de la clé publique, d'un pointeur (8) dans la table de certificats vers le condensé de la clé publique (R_p) de l'entité de certification qui a émis le certificat (<R,B>) de la clé publique à insérer, de manière à définir un arbre de certification.

4. Procédé selon la revendication 3,
caractérisé en ce qu'il comprend une phase (3) de suppression d'un condensé (Hash(B_p)) de clé publique (B_p) dans la table de certificats (5, 5') consistant à supprimer de la table de certificats le condensé d'une clé publique à retirer, et à supprimer tous les condensés de clés publiques de la table de certificats associés à un pointeur (8) indiquant la clé publique (B_p) à retirer.

5. Procédé selon l'une des revendications 2 à 4,
caractérisé en ce que chaque condensé de clé publique inscrit dans la table de certificats (5, 5') est associé à une date de fin de validité (7), et en ce que la phase (1) d'insertion d'une clé publique (B_p) dans la table de certificats comprend en outre des étapes consistant à lire dans le certificat (<R,B>) reçu une date de fin de validité de la clé publique à insérer, et à inscrire dans la table de certificats, en association avec le condensé de la clé publique à insérer, la date de fin de validité de la clé publique (B_p) à insérer, si elle est antérieure à la date de fin de validité de la clé publique (R_p) de l'entité de certification lue dans la table de certificats.

6. Procédé selon l'une des revendications 2 à 5,
caractérisé en ce que chaque condensé de clé publique inscrit dans la table de certificats (5, 5) est associé à un compteur (41) d'utilisation qui est incrémenté à chaque fois qu'une signature électronique est vérifiée à l'aide de la clé publique, et en ce qu'il comprend la suppression d'un condensé de clé publique dans la table de certificats lorsque le compteur d'utilisation est nul et que le nombre d'emplacements vides dans la table de certificats est inférieur à un seuil

prédéterminé.

7. Procédé selon l'une des revendications 2 à 6, caractérisé en ce que chaque condensé de clé publique inscrit dans la table de certificats (5, 5') est associé à un compteur (41) d'utilisation qui est incrémenté à chaque fois qu'une signature électronique est vérifiée à l'aide de la clé publique, à une date de dernière utilisation (42) qui est mise à jour à chaque fois que le compteur d'utilisation associé est incrémenté, et en ce que lorsque le nombre d'emplacements vides dans la table de certificats est inférieur à un seuil prédéterminé, il comprend en outre une étape de sélection d'un condensé de clé publique à supprimer en fonction des valeurs respectives associées du compteur d'utilisation et de la date de dernière utilisation.

8. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que pour calculer des formes condensées de clés publiques, le microcircuit (53) utilise une fonction de hachage prédéfinie.

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce qu'il comporte une phase d'insertion d'une clé publique racine (R_p) dans la table de certificats (5, 5'), cette phase d'insertion étant effectuée par un traitement d'écriture contrôlée par un MAC calculé à l'aide d'une clé spécifique du microcircuit (53) et connue uniquement d'une entité émettrice du microcircuit.

10. Procédé selon l'une des revendications 1 à 9, caractérisé en ce que le condensé d'une clé publique mémorisé dans la table de certificats (5, 5') est obtenu en calculant un condensé de la clé publique associée à d'autres informations comme la date de fin de validité de la clé publique, des informations d'identité, et de numéros de série, ces informations étant transmises au microcircuit (53) à chaque vérification de signature à l'aide de la clé publique.

11. Procédé selon l'une des revendications 1 à 10, caractérisé en ce que le condensé d'une clé publique mémorisé dans la table de certificats (5, 5') est obtenu en calculant un condensé du certificat reçu par le microcircuit (53) lors de l'insertion de la clé publique dans la table de certificats, ce certificat étant transmis au microcircuit à chaque vérification de signature à l'aide de la clé publique.

12. Procédé selon l'une des revendications 1 à 11, caractérisé en ce que la table de certificats (5, 5') est stockée dans une zone mémoire sécurisée du microcircuit (53).

13. Carte à microcircuit (53), caractérisée en ce qu'elle met en œuvre le procédé selon l'une des revendications 1 à 12.

14. Système de vérification de signature électronique comprenant un microcircuit (53) connectable à un système de traitement de données (51), caractérisé en ce qu'il comprend des moyens pour en œuvre le procédé selon l'une des revendications 1 à 12.

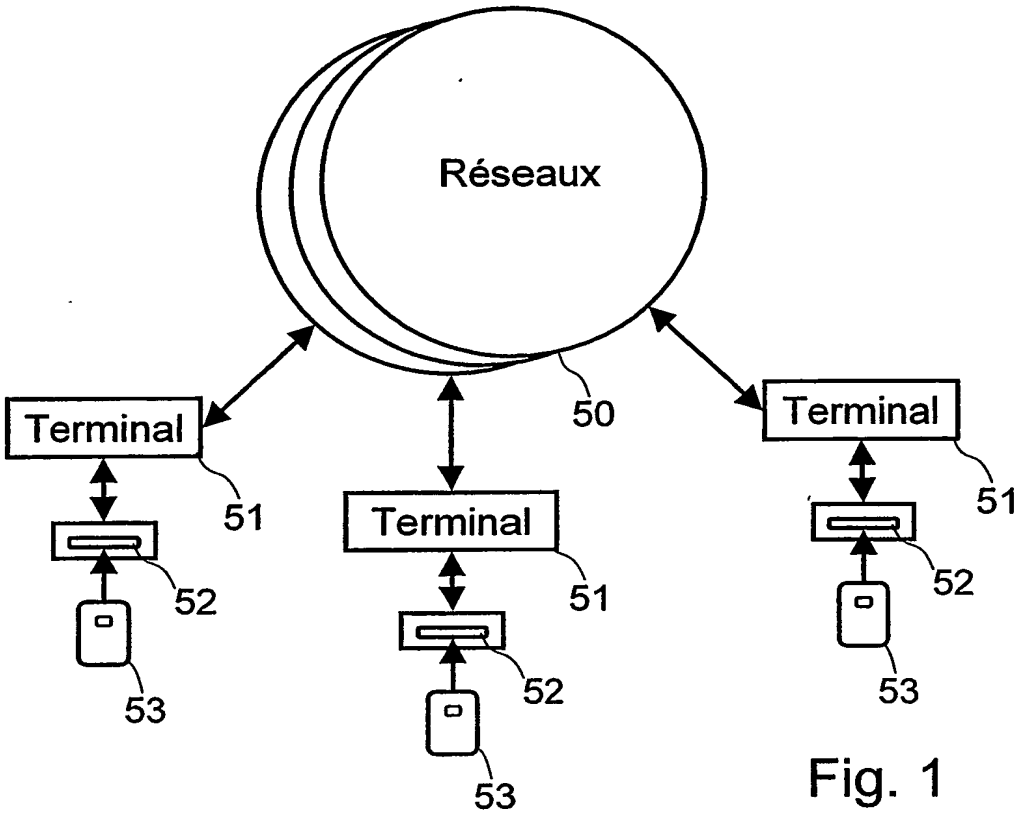


Fig. 1

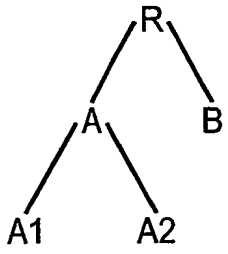


Fig. 2

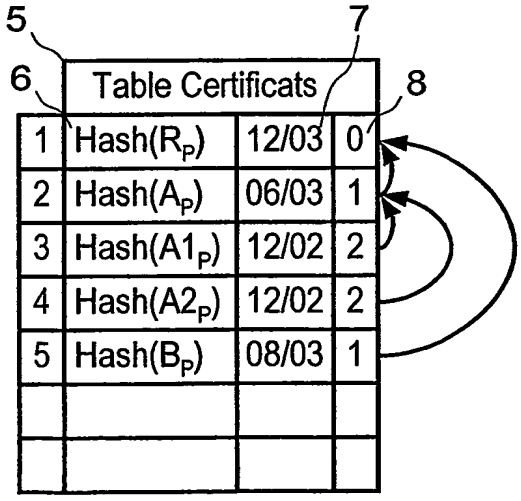


Fig. 3

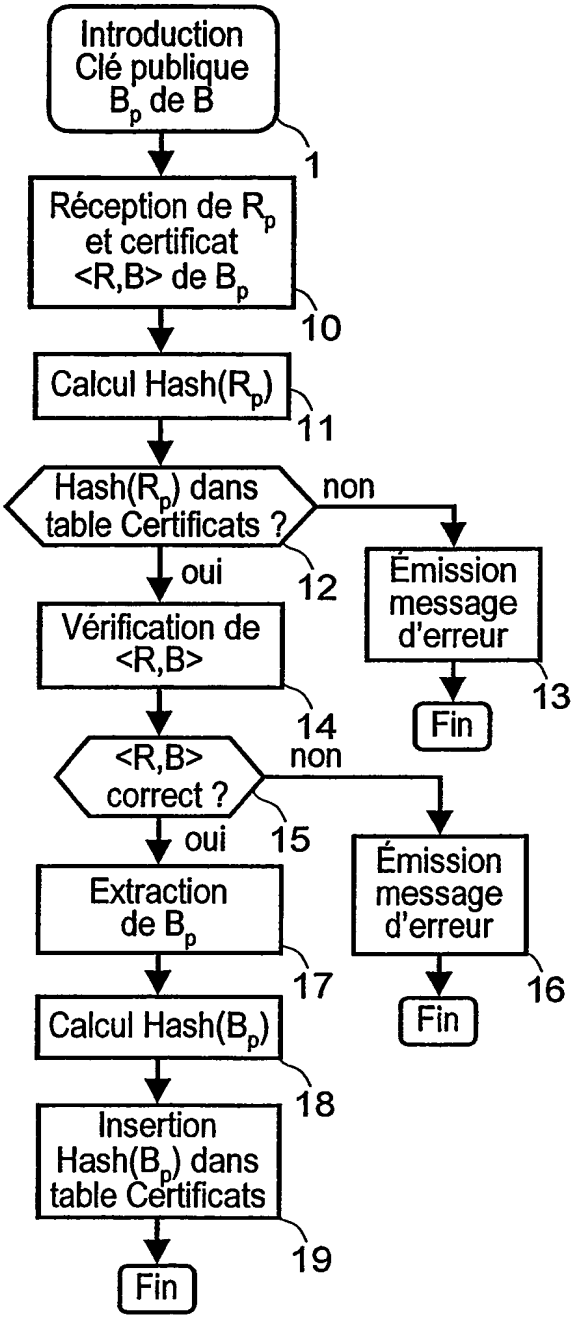

Introduction Clé publique B_p de B
1
Réception de R_p et certificat <R,B> de B_p
10
Calcul Hash(R_p)
11
Hash(R_p) dans table Certificats ?
non
12
oui
Émission message d'erreur
13
Fin
Vérification de <R,B>
14
<R,B> correct ?
non
15
oui
Émission message d'erreur
16
Fin
Extraction de B_p
17
Calcul Hash(B_p)
18
Insertion Hash(B_p) dans table Certificats
19
Fin

Fig. 4

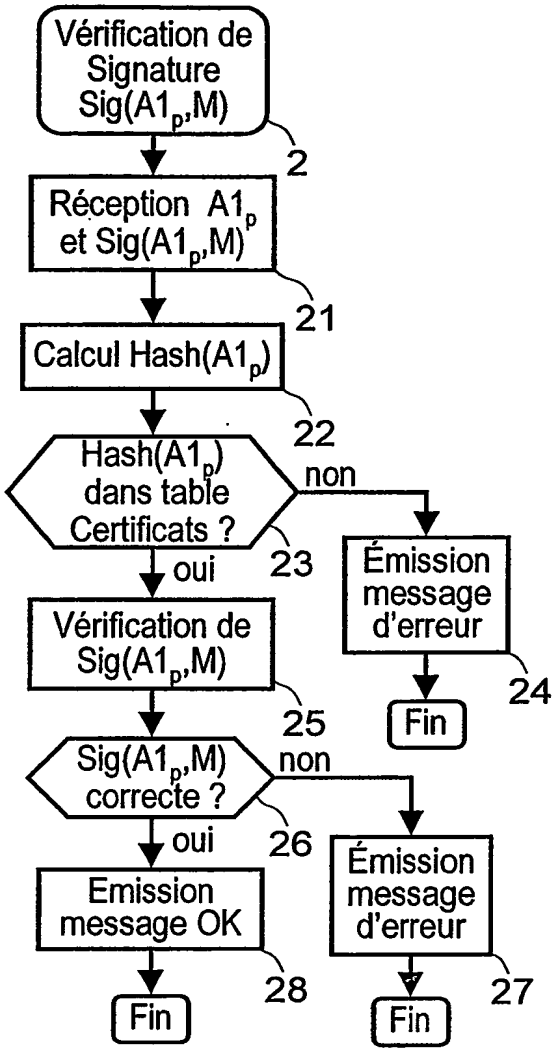

Vérification de Signature Sig($A1_p$,M)
2
Réception $A1_p$ et Sig($A1_p$,M)
21
Calcul Hash($A1_p$)
22
Hash($A1_p$) dans table Certificats ?
non
23
oui
Émission message d'erreur
24
Fin
Vérification de Sig($A1_p$,M)
25
Sig($A1_p$,M) correcte ?
non
26
oui
Émission message d'erreur
27
Fin
Emission message OK
28
Fin

Fig. 5

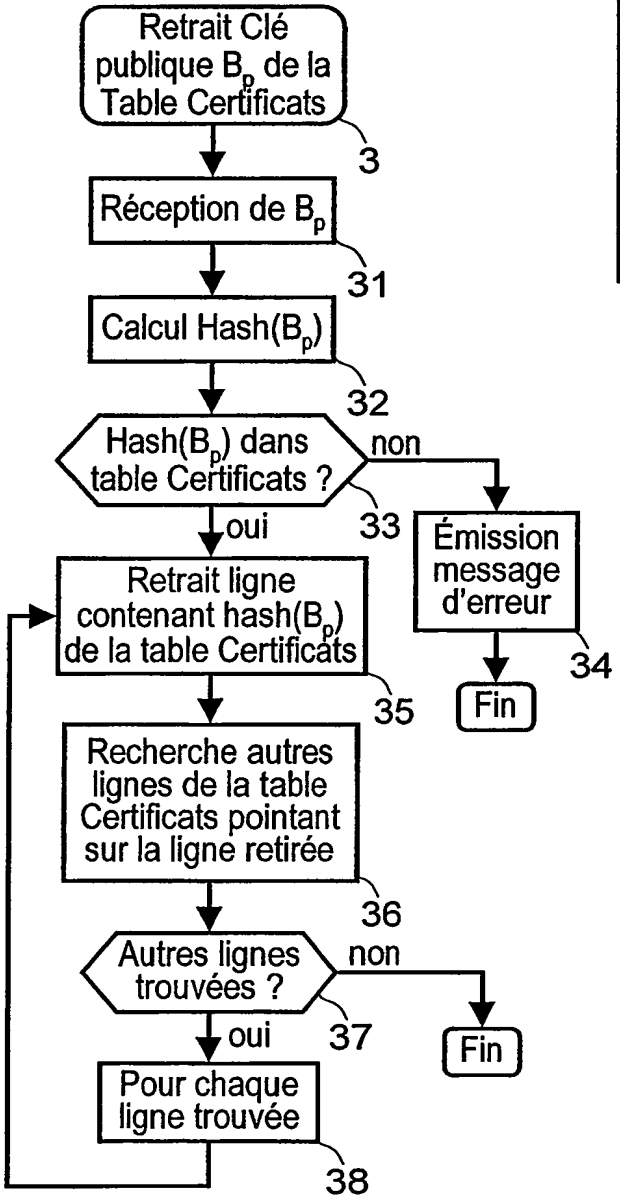

Retrait Clé publique B_p de la Table Certificats
3
Réception de B_p
31
Calcul Hash(B_p)
32
Hash(B_p) dans table Certificats ?
non
33
oui
Émission message d'erreur
34
Fin
Retrait ligne contenant hash(B_p) de la table Certificats
35
Recherche autres lignes de la table Certificats pointant sur la ligne retirée
36
Autres lignes trouvées ?
non
37
oui
Fin
Pour chaque ligne trouvée
38

Fig. 6

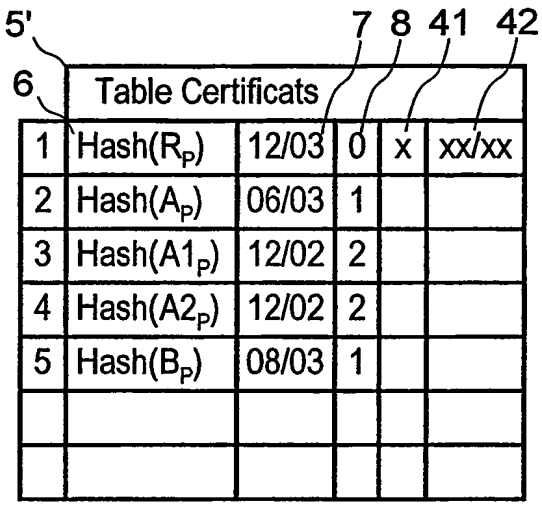

5'
6
7
8
41
42
Table Certificats
1 Hash(R_P) 12/03 0 x xx/xx
2 Hash(A_P) 06/03 1
3 Hash($A1_P$) 12/02 2
4 Hash($A2_P$) 12/02 2
5 Hash(B_P) 08/03 1

Fig. 7

INTERNATIONAL SEARCH REPORT

International Application No
PCT 03/01535

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 856 821 A (NIPPON TELEGRAPH & TELEPHONE) 5 August 1998 (1998-08-05) abstract column 5, line 57 -column 6, line 29	1,13,14
A	WO 01 52470 A (CORELLA FRANCISCO ;HEWLETT PACKARD CO (US)) 19 July 2001 (2001-07-19) page 47, line 21 -page 50, line 15	1
A	US 6 215 872 B1 (VAN OORSCHOT PAUL C) 10 April 2001 (2001-04-10) column 4, line 11 - line 21 column 8, line 60 -column 9, line 8	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 October 2003	24/10/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/03/01535

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0856821 A	05-08-1998	JP 3082882 B2	28-08-2000
		JP 6103425 A	15-04-1994
		JP 3082883 B2	28-08-2000
		JP 6103426 A	15-04-1994
		JP 3080202 B2	21-08-2000
		JP 6162289 A	10-06-1994
		JP 3085334 B2	04-09-2000
		JP 6162287 A	10-06-1994
		JP 6161354 A	07-06-1994
		EP 0856821 A2	05-08-1998
		EP 0856822 A2	05-08-1998
		DE 69322463 D1	21-01-1999
		DE 69322463 T2	10-06-1999
		DE 69332745 D1	10-04-2003
		EP 0588339 A2	23-03-1994
		US 5396558 A	07-03-1995
		US 5446796 A	29-08-1995
		US 5502765 A	26-03-1996
WO 0152470 A	19-07-2001	US 2001032310 A1	18-10-2001
		AU 2792801 A	24-07-2001
		EP 1250774 A2	23-10-2002
		WO 0152470 A2	19-07-2001
US 6215872 B1	10-04-2001	US 6134327 A	17-10-2000
		US 6092201 A	18-07-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PC[redacted] 03/01535

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, EPO-Internal, PAJ, INSPEC, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 856 821 A (NIPPON TELEGRAPH & TELEPHONE) 5 août 1998 (1998-08-05) abrégé colonne 5, ligne 57 -colonne 6, ligne 29	1,13,14
A	WO 01 52470 A (CORELLA FRANCISCO ;HEWLETT PACKARD CO (US)) 19 juillet 2001 (2001-07-19) page 47, ligne 21 -page 50, ligne 15	1
A	US 6 215 872 B1 (VAN OORSCHOT PAUL C) 10 avril 2001 (2001-04-10) colonne 4, ligne 11 - ligne 21 colonne 8, ligne 60 -colonne 9, ligne 8	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
10 octobre 2003	24/10/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/03/01535

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0856821	A	05-08-1998	JP	3082882 B2	28-08-2000
			JP	6103425 A	15-04-1994
			JP	3082883 B2	28-08-2000
			JP	6103426 A	15-04-1994
			JP	3080202 B2	21-08-2000
			JP	6162289 A	10-06-1994
			JP	3085334 B2	04-09-2000
			JP	6162287 A	10-06-1994
			JP	6161354 A	07-06-1994
			EP	0856821 A2	05-08-1998
			EP	0856822 A2	05-08-1998
			DE	69322463 D1	21-01-1999
			DE	69322463 T2	10-06-1999
			DE	69332745 D1	10-04-2003
			EP	0588339 A2	23-03-1994
			US	5396558 A	07-03-1995
			US	5446796 A	29-08-1995
			US	5502765 A	26-03-1996
WO 0152470	A	19-07-2001	US	2001032310 A1	18-10-2001
			AU	2792801 A	24-07-2001
			EP	1250774 A2	23-10-2002
			WO	0152470 A2	19-07-2001
US 6215872	B1	10-04-2001	US	6134327 A	17-10-2000
			US	6092201 A	18-07-2000